



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/723,675	11/26/2003	Charles Cameron Brackett	133630IT/YOD GEMS:0237	8884
68174	7590	04/28/2008	EXAMINER	
GE HEALTHCARE c/o FLETCHER YODER, PC P.O. BOX 692289 HOUSTON, TX 77269-2289			PATEL, NIRAV B	
			ART UNIT	PAPER NUMBER
			2135	
			MAIL DATE	DELIVERY MODE
			04/28/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/723,675	<b>Applicant(s)</b> BRACKETT ET AL.	
	<b>Examiner</b> NIRAV PATEL	<b>Art Unit</b> 2135	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 08 January 2008.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on Jan 10, 2008 has been entered.

2. Claims 1-29 are pending. Claims 1-4, 6-17, 19-28 are amended and Claim 29 is newly added by the applicant.

### Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

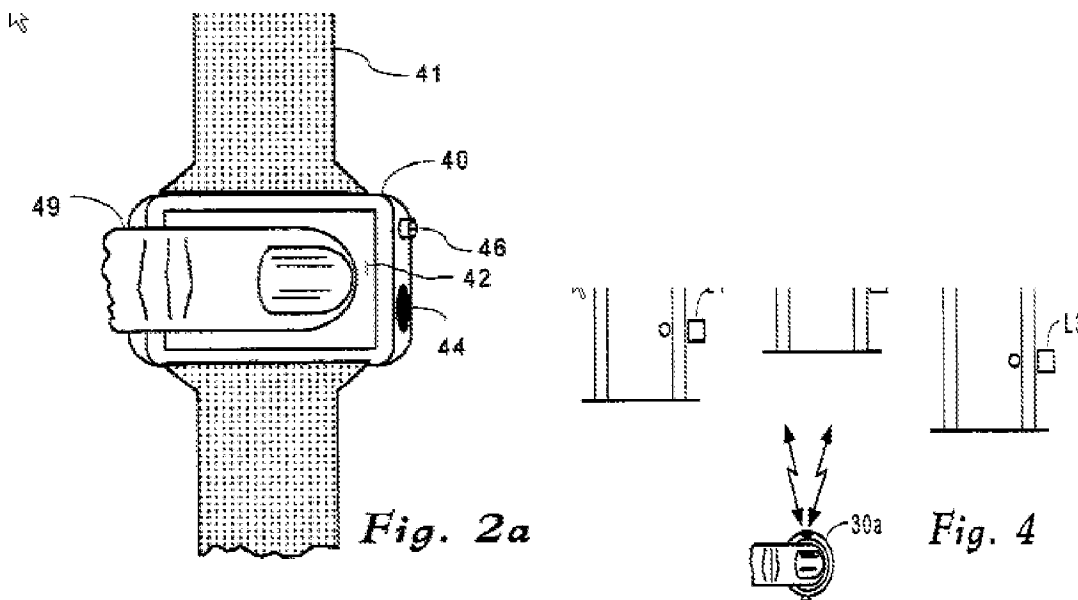
(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 2, 3, 5, 9, 10, 12, 15-18 and 23-28 are rejected under 35 U.S.C. 102 (e) as being anticipated by Hamid et al. (US Patent No. 6,877,097).

As per claim 1, Hamid ('097) discloses:

a method for authentication and log-in to a system [col. 9 lines 62-65, **"A user is provided with a number of functions each accessible by transmission of a unique access code for executing that function"**, col. 10 line 2 **"logging into a computer system"**], comprising: performing a biometric scan of a user with a wireless biometric device comprising a wireless proximity detection

device coupled to a biometric device [Figs. 2, 2a, col. 7 lines 24-41, “a biometric sensor in the form of capacitive array for sensing biometric characteristics of any of a person's digit tips. A fingertip 49 is shown positioned against the platen 42, as it would be for sensing of the finger's print. A processor, not shown, analyzes the finger print and may cause an authorization signal to be transmitted through an infrared port 44”, Figs. 3, 4];



comparing the biometric scan of the user to stored biometric data to authenticate the user [Figs. 3, 5a col. 7 lines 42-67, 1-15 “a sensor array or scanner unit 52, for sensing a fingertip pattern or some other biometric characteristic”, “The RAM 56 has also been written with a record of a finger print characteristic of the intended user. In operation the processor 50 fetches a segment representative of a central row portion of the finger print characteristic from the RAM 56 and progressively compares the segment with a serial nondestructive row by row readout from the data buffer 54”]; and authenticating the user via the wireless biometric device [Fig. 5, col. 8 lines 1-10 “the finger print characteristic from the RAM 56 is compared row segment after

Art Unit: 2135

**row segment from beginning to end with the binary code stored in a data buffer 54 to recognize any apparent corresponding segments”];** and communicating with the system via the wireless proximity detection device only after authenticating the user **[Fig. 5, col. 8 lines 10-18 “....reference position until in any one such pass a sufficient number of row segments with apparent matches are realized to warrant a transmission of a predetermined authorization signal. If there are an insufficient number of apparently matching segments, transmission of an authorization signal is unwarranted”, Fig. 3, 4, i.e. communicating with the system *only after authenticating* the user].**

As per claim 2, the rejection of claim 1 is incorporated and Hamid ('097) discloses:

detecting the authenticated user and logging the user into the system **[col.8 lines 10-18, “....reference position until in any one such pass a sufficient number of row segments with apparent matches are realized to warrant a transmission of a predetermined authorization signal. If there are an insufficient number of apparently matching segments, transmission of an authorization signal is unwarranted”, col. 9 lines 62-65, col. 10 lines 1-3 “transmission of a unique access code for executing that function”, col. 10 line 2 “logging into a computer system”].**

As per claim 3, the rejection of claim 1 is incorporated and Hamid ('097) discloses:

sending a signal to the system from the wireless biometric device to log the user into the system **[col.8 lines 10-18, “....reference position until in any one such pass a sufficient number of row segments with apparent matches are realized to warrant a transmission of a predetermined**

**authorization signal. If there are an insufficient number of apparently matching segments, transmission of an authorization signal is unwarranted”, col. 9 lines 62-65, col. 10 lines 1-3 “transmission of a unique access code for executing that function”, col. 10 line 2 “logging into a computer system”].**

As per claim 5, the rejection of claim 1 is incorporated and Hamid ('097) discloses:

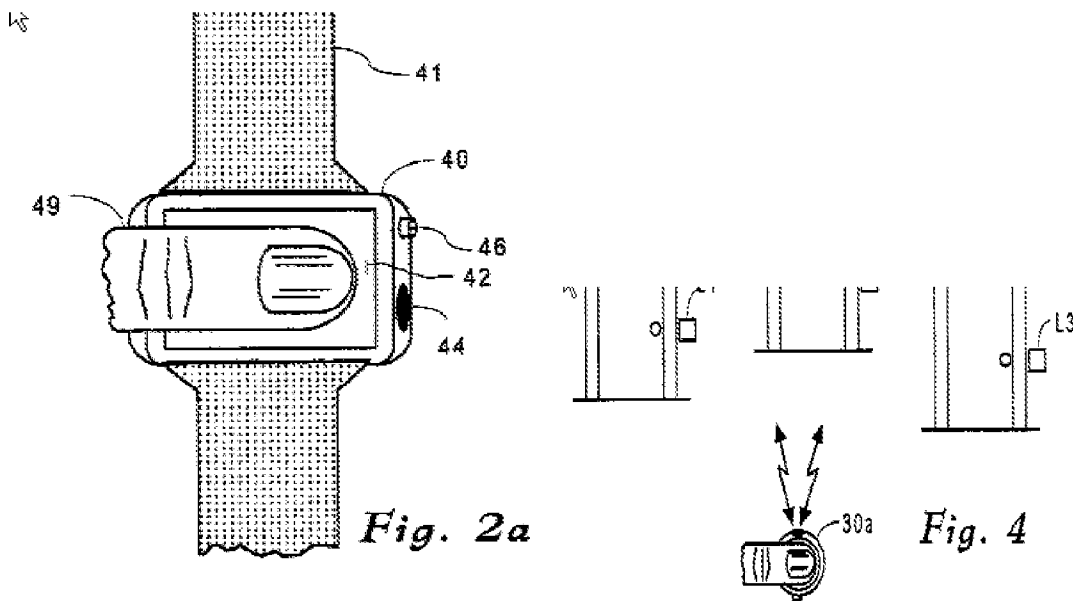
the biometric scan comprises at least one of a thumbprint scan, a fingerprint scan, a handprint scan, a retinal scan, a voice recognition, or a facial recognition **[Fig. 2a, 3]**.

As per claim 9, Hamid ('097) discloses:

a method of accessing a system, comprising: scanning a user with a wireless biometric device **[col. 7 lines 42-44, col. 9 lines 62-67, col. 10 lines 1-11, Fig. 2a, 4]**; recognizing biometric measurements of the user and authenticating the user at the wireless biometric device to permit access by the user to the system **[Fig. 5, col. 7 lines 52-67, “...In operation the processor 50 fetches a segment representative of a central row portion of the finger print characteristic from the RAM 56 and progressively compares the segment with a serial nondestructive row by row readout from the data buffer 54” col. 8 lines 1-16 “the finger print characteristic from the RAM 56 is compared row segment after row segment from beginning to end with the binary code stored in a data buffer 54 to recognize any apparent corresponding segments” “....reference position until in any one such pass a sufficient number of row segments with apparent matches are realized to warrant a transmission of a predetermined authorization signal. If there are an insufficient**

Art Unit: 2135

number of apparently matching segments, transmission of an authorization signal is unwarranted”];



sending a wireless signal from the wireless biometric device to a system device of the system after authenticating the user to detect the system and to provide a user identification code to the system [Fig. 5, col. 8 lines 11-18, “....reference position until in any one such pass a sufficient number of row segments with apparent matches are realized to warrant a transmission of a predetermined authorization signal. If there are an insufficient number of apparently matching segments, transmission of an authorization signal is unwarranted” Fig. 6, col. 9 lines 62-67, col. 10 lines 1-3 i.e. sending the signal to the system *after authenticating the user* to detect the system and to provide a user identification code]; and logging the user into the system based on the user identification code [Fig. 6, col. 9 lines 62-67, “A user is provided with a number of functions each accessible by transmission of a unique access code for executing that function”, col. 10 lines 1-3 “logging into a computer system”].

As per claim 10, the rejection of claim 9 is incorporated and Hamid ('097) discloses:

the system device is an antenna configured to receive a wireless signal **[col. 7 lines 36-38]**.

As per claim 12, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 15, Hamid ('097) discloses:

A method of logging into a system, comprising: activating a proximity detection device only after satisfying a required biometric authentication at the proximity detection device **[Fig. 5, col. 7 lines 52-67, col. 8 lines 1-18, “....reference position until in any one such pass a sufficient number of row segments with apparent matches are realized to warrant a transmission of a predetermined authorization signal. If there are an insufficient number of apparently matching segments, transmission of an authorization signal is unwarranted” Fig. 6** i.e. activating the device only after satisfying a required biometric authentication at the device]; transmitting user identification data from the proximity detection device to the system via a wireless connection; and logging a user into the system **[Fig. 5, col. 8 lines 13-16, Fig. 6, col. 9 lines 62-67, col. 10 lines 1-3]**.



Art Unit: 2135

As per claim 16, the rejection of claim 15 is incorporated and Hamid ('097) discloses: wherein activating the proximity detection device comprises scanning a user with a biometric device integrated with the wireless proximity detection device **[Fig. 2a, 3]**.

As per claim 17, the rejection of claim 16 is incorporated and Hamid ('097) discloses: biometric authentication comprises comparing biometric measurements of the user to stored measurement data **[Fig. 5, col. 7 lines 62-67, col. 8 lines 1-15]**.

As per claim 18, the rejection of claim 16 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 23, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 24, it encompasses limitations that are similar to limitations of claim 9. Thus, it is rejected with the same rationale applied against claim 9 above.

As per claim 25, it encompasses limitations that are similar to limitations of claim 15. Thus, it is rejected with the same rationale applied against claim 15 above.

Art Unit: 2135

As per claim 26, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 27, it encompasses limitations that are similar to limitations of claim 9. Thus, it is rejected with the same rationale applied against claim 9 above.

As per claim 28, it encompasses limitations that are similar to limitations of claim 15. Thus, it is rejected with the same rationale applied against claim 15 above.

### **Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 4, 11, 20, 21, 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamid et al (US Patent No. 6,877,097) and in view of Uchida (US Patent No. 6,751,734).

As per claim 4, the rejection of claim 1 is incorporated and Hamid ('097) teaches sending the authorization signal/access code to a system interface antenna [col. 7 lines 36-38, **“an antenna may be combined with the wrist strap 41 for radio frequency transmission of the authorization signal”**, col. 8 lines 14-16 **“apparent matches are realized to warrant a transmission of a**

**predetermined authorization signal”, col. 9 lines 62-65].** Further, Hamid ('097) teaches transmitting the authorization signal/access code and logging into the system **[col. 9 lines 62-65, col. 10 line 2, Fig. 4, 6].**

Hamid ('097) doesn't expressively mention *comparing* the user identification information to an appropriate user database to log the user into the system.

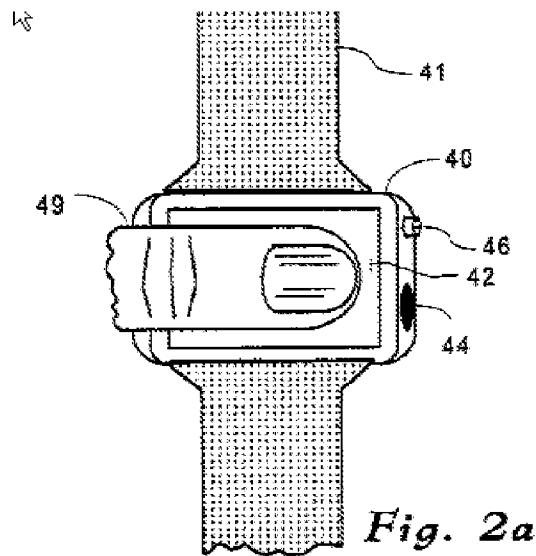
Uchida teaches sending user identification information and comparing the user identification information to an appropriate user database to log the user into the system **[Fig. 1, 3, col. 10 lines 7-15, “the authentication executing device 2, the communication message from the portable terminal 1 is received by the communication message receiving unit 21 (Step 301), which sends the same message to the authentication message decrypting unit 23” col. 11 lines 9-12, 23-26, “After decrypting the data in the authentication message decrypting unit 23, the PC performs the log-in operation using the user name and log-in password”, col. 11 lines 59-64 “the authentication host examines the coincidence between the same information and the information stored therein, thereby to confirm the personal identity”].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Uchida with Hamid ('097) to compare the user identification information at the receiver side, since one would have been motivated to provide an authentication mechanism with high security, free from a trouble of remembering a password **[Uchida, col. 2 lines 11-14].**

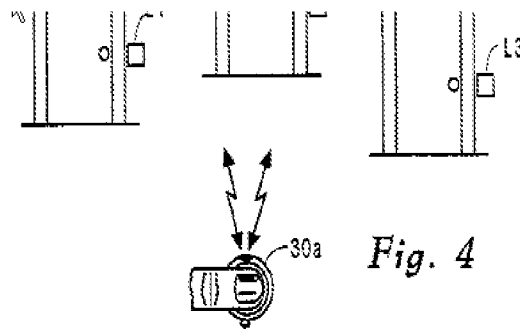
As per claim 11, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

As per claim 20, Hamid ('097) discloses:

An authentication and log-in system for accessing a secured system, comprising: a wireless biometric device comprising a wireless proximity detection pin coupled to a biometric device; a sensor disposed in the biometric device for performing a biometric measurement of a user **[Fig. 2a, 3 col. 7 lines 24-45 “the portable fingerprint device is housed in an ubiquitous object, in this example within a housing 40 of a functional wristwatch which is typically secured to a person's wrist by a watch band 41. A front face of the housing 40 is a transparent platen 42 which provides a view of an underlying timepiece display, not shown, as well as carrying a biometric sensor in the form of capacitive array for sensing biometric characteristics of any of a person's digit tips. A fingertip 49 is shown positioned against the platen 42, as it would be for sensing of the finger's print. A processor, not shown, analyzes the finger print and may cause an authorization signal to be transmitted through an infrared port 44. In a different arrangement an antenna may be combined with the wrist strap 41 for radio frequency transmission of the authorization signal” “a sensor array or scanner unit 52, for sensing a fingertip pattern or some other biometric characteristic”];**



a processing module disposed within the wireless biometric device for conducting the biometric measurement of the user, authenticating the user [Fig. 5, col. 7 lines 42-67, col. 8 lines 1-15 “the finger print characteristic from the RAM 56 is compared row segment after row segment from beginning to end with the binary code stored in a data buffer 54 to recognize any apparent corresponding segments” “....reference position until in any one such pass a sufficient number of row segments with apparent matches...”], and transmitting a wireless communication only after authenticating the user to detect the secured system and to provide an authenticated user identification code to the secured system [Fig. 5, col. 8 lines 13-18, “....reference position until in any one such pass a sufficient number of row segments with apparent matches are realized to warrant a transmission of a predetermined authorization signal. If there are an insufficient number of apparently matching segments, transmission of an authorization signal is unwarranted” Fig. 6, col. 9 lines 62-65, col. 10 line 2 i.e. transmitting the signal to the system *after authenticating the user* to detect the system and to provide a user identification code];



a device disposed in the secured system for receiving the authenticated user identification code **[Fig. 4, 6]**.

Hamid ('097) teaches transmitting the authorization signal/access code and logging into the system **[col. 9 lines 62-65, col. 10 line 2, Fig. 4, 6]**.

Hamid ('097) doesn't expressively mention *comparing* the authenticated user identification code to a stored identification code and for logging the user into the secured system.

Uchida teaches receiving the authenticated user identification code and *comparing* the authenticated user identification code to a stored identification code and for logging the user into the secured system **[Fig. 1, 3, col. 10 lines 7-15, “the authentication executing device 2, the communication message from the portable terminal 1 is received by the communication message receiving unit 21 (Step 301), which sends the same message to the authentication message decrypting unit 23” col. 11 lines 9-12, 23-26, “After decrypting the data in the authentication message decrypting unit 23, the PC performs the log-in operation using the user name and log-in password”, col. 11 lines 59-64 “the authentication host examines the coincidence between the same information and the information stored therein, thereby to confirm the personal identity”]**.

Art Unit: 2135

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Uchida with Hamid ('097) to compare the user identification information at the receiver side, since one would have been motivated to provide an authentication mechanism with high security, free from a trouble of remembering a password **[Uchida, col. 2 lines 11-14]**.

As per claim 21, the rejection of claim 20 is incorporated and Hamid ('097) discloses:

the biometric scan comprises at least one of a thumbprint scan, a fingerprint scan, a handprint scan, a retinal scan, a voice recognition, or a facial recognition **[Fig. 2a, 3]**.

As per claim 29, the rejection of claim 20 is incorporated and Hamid ('097) discloses:

the wireless detection pin comprises a Bluetooth mobility pin **[Fig. 2 component 34 or Fig. 2a component 44]**.

5. Claims 6, 13 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamid et al (US Patent No. 6,8,77,097) and in view of Wong et al (US Patent No. 6,260,021).

As per claim 6, the rejection of claim 1 is incorporated and Hamid ('097) discloses authenticating and log-in to the system (e.g. computer system, engaging security system....etc.) **[col. 10 lines 62-65, col. 10 lines 1-3]**. Hamid doesn't expressively mention a picture and archival communication system (PACS) and a PACS workstation.

Art Unit: 2135

Wong teaches: a system comprises a picture and archival communication system and an interface of the system comprises a PACS workstation **[Fig. 1 component 14, 26 or Fig. 2]**. Further, Wong teaches the authorization process for providing the user access to the system **[Fig. 4]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wong with Hamid ('097), since one would have been motivated to enable the uniform access to and ready distribution of medical images and associated records **[Wong, col. 1 lines 8-9]** and to provide automated security for permitting access to a service or a system by a designated person **[Hamid, col. 1 lines 4-6]**.

As per claim 13, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

As per claim 19, the rejection of claim 15 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

6. Claims 7, 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamid et al (US Patent No. 6,8,77,097) and in view of Kuth (US Patent No. 6,684,093).



Art Unit: 2135

As per claim 7, the rejection of claim 1 is incorporated and Hamid ('097) discloses authenticating and log-in to the system (e.g. computer system, engaging security system....etc.) **[col. 10 lines 62-65, col. 10 lines 1-3]**. Hamid ('097) doesn't expressively mention a medical modality system and an interface of the system comprises an operator interface of the medical modality system.

Kuth teaches: the system comprises a medical modality system and the interface of the system comprises an operator interface of the medical modality system **[Fig. 1]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kuth with Hamid ('097), since one would have been motivated to prevent the incorrect assignment of the data **[Kuth, col. 1 lines 19-22]** and to provide automated security for permitting access to a service or a system by a designated person **[Hamid ('097), col. 1 lines 4-6]**.

As per claim 8, the rejection of claim 7 is incorporated and Kuth teaches the medial modality system is an imaging system **[Fig. 1]**.

As per claim 14, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 7. Thus, it is rejected with the same rationale applied against claim 7 above.

7. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hamid et al (US Patent No. 6,877,097) in view of Uchida (US Patent No. 6,751,734) and in view of Wong et al (US Patent No. 6,260,021).

Art Unit: 2135

As per claim 22, the rejection of claim 20 is incorporated and Hamid ('097) discloses authenticating and log-in to the system (e.g. computer system, engaging security system....etc.) **[col. 10 lines 62-65, col. 10 lines 1-3]**. Hamid ('097) and Uchida don't expressively mention a picture and archival communication system (PACS) and a PACS workstation.

Wong teaches: a system comprises a picture and archival communication system and an interface of the system comprises a PACS workstation **[Fig. 1 component 14, 26 or Fig. 2]**. Further, Wong teaches the authorization process for providing the user access to the system **[Fig. 4]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wong with Hamid ('097) and Uchida, since one would have been motivated to enable the uniform access to and ready distribution of medical images and associated records **[Wong, col. 1 lines 8-9]** and to provide automated security for permitting access to a service or a system by a designated person **[Hamid ('097), col. 1 lines 4-6]**.

### Response to Argument

8. This written action is responding to the Request for Continued Examination (RCE) dated Jan. 10, 2008.

Applicant has amended claims 26-28 to correct the 35 U.S.C. 101 issue. The amended claims have overcome such deficiency. Therefore, the rejection under 35 U.S.C. 101 has been withdrawn.

Applicant has amended claims 1, 9, 15, 20, 23-28 and added new claim 29, which necessitated new ground of rejection. See new ground of rejection above based on **newly cited prior art (Hamid et al – US 6,877,097)** and in combination with various previously cited prior art. Therefore, the applicant's arguments, filed on Jan. 10, 2008, are moot in view of the new ground(s) of rejection.

Regarding to applicant argument to the claim limitation “communicating with the system.....*only after authenticating the user*” and “activating a proximity detection device *only after satisfying a required biometric authentication at the proximity detection system*”, the **newly cited reference** **(Hamid et al – US 6,877,097)** teaches the claim limitation as above (See detail rejection above).

### Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hashimoto et al (US 2003/0159040) – Method and Apparatus for personal identification

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

*NP*

*3/17/08*

*/KIMYEN VU/*

*Supervisory Patent Examiner, Art Unit 2135*